Homework #1 – CS6823 – Network Security

Directions: Keep your answers as short as possible. Most subquestion should be answered in no more one sentence. This assignment is based on Lecture 1 and 2. Do cite your sources if you use other than the lecture slides. Answers are in black color.

1. [5 pts] Define these terms: **Confidentiality**, **Integrity**, **Availability**, **Authenticity**, and **Non-Repudiation**.

   The answers use Entity as the focus (information, message, packets or anything)
   - ***Confidentiality:***
     Having an entity hidden (secretive or unexposed) from unauthorized access or users with restricted access
   - ***Integrity:***
     Making sure that the entity has not been tampered with in course of delivery
   - ***Availability:***
     Having the service always available at any circumstance (During Attack or Scaled Usage)
   - ***Authenticity:***
     Making sure the origin of data is as mentioned in the information or Making sure if the origin and the source details in the entity are same.
   - ***Non-Repudiation:***
     Making sure a valid origin as well as integrity of the entity

   Reference: Lecture Slides

2. [8 pts] What's the difference between:
   a. ***Risk*** *and* ***Threat***
   Risk *is a probability to lose or compromise (due to negative event) an entity causing certain amount of loss to the value*
   Threat *is the possibility of an act that would successfully accomplish what would be considered a risk (Negative Event) causing loss to the value of the entity*

   b. ***Vulnerability*** *and* ***Exploit***
   Vulnerability *is the measure of efficiency of a system corresponding to the probability of a threat occurrence*
   Exploit *is an activity that would trigger conditions (to hit a vulnerability) for a threat to occur*

   Reference: Lecture Slides

3. [4 pts] Define **Likelihood** and **Consequence** (also called impact)
   - ***Likelihood:*** *It is the rate or probability at which some event may occur*
   - ***Consequence:*** *It is the adverse effects or loss that would be incurred due to occurrence of an event.*

   Reference: Lecture Slides

4. [4 pts] On the slide titled "Example Risk Matrix (from the DoD)," does example #1 reduce likelihood or consequence? How?
   The example 1: reduces the likelihood. The consequence of a buffer overflow remains the same while the likelihood is reduced by spending money to hire more skilled resources to work on the software to reduce buffer overflow bugs (Less occurrence of Buffer Overflow bugs)

   Reference: Lecture Slides

5. [6 pts] Suppose a credit card company gets compromised once every four years and one million credit cards numbers each time. The cost of replacing credit cards, charge-back fraud, and fraud is ten million dollars. How much can the credit card company spend each year on prevention of being compromised if it guarantees the company won't be hacked anymore?
   Anything less than 2500000 (2.5 Million) dollars would guarantee the company won't be hacked.

   Reference: Lecture Slides

6. [6 pts] In the lecture 1 slide titled "Cost of an Attack" (attack trees) what is the most expensive attack(s)? What is the cheapest attack(s)?
   - *Expensive Attack: 100K – Install Improperly / Blackmail*
   - *Cheap Attack: 10K – Cut Open the Safe*

   Reference: Lecture Slides

7. [6 pts] List **three** Google hacking keywords with an example of each.
   - **Site ->** site:cloudshark.org/captures# password – *Searching for password in packet captures*
   - **Inurl, intext ->** inurl:github.com intitle:config intext:"password" – Searching for *Config files in Github with password*
   - **Link->** link:www.nyu.edu intext:"schedule" – *Searches for links with schedule in nyu domain*
   - **Related->** related:nyupoly – *various Links of NYU Poly school*
   - **Filetype ->** filetype:asmx inurl:(_vti_bin|api|webservice) – *Return any running web service*
   - **InTitle ->** intitle:index.of inurl:grades site:edu – *Sensitive directories containing grades*

   Reference: https://www.exploit-db.com/ghdb/

8. [6 pts] Describe **three technical** and **three non-technical** ways to perform reconnaissance on a company.
   - ***Technical:***
     **Get Web Servers and IP Address information of the company using DNS Dig or Lookup the whois DB*
     *******Reading through the company's social posts and social accounts.*
     **Connect with the employees through social networks and gain trust for company info*
     *******Perform google hacks or searches – Google hack keywords for any sensitive information*
     **Go through the securities of the company and Job Postings*

   - ***Non-Technical:***
     **Apply for interview and get access to the company inside*

**Buy Stocks in the company and get access to the company insider information and decisions*
**Stand by the company location to talk or eavesdrop to any employees or hangout with any*
**Collect the waste thrown by the company outside premises for any important papers.*
**Enquire to the security showing up as a courier person or package delivery person*

Reference: Lecture Slides

9. [6 pts] Describe what each of the following DNS records are:
   a. A Record – Maps the Domain Name to the corresponding IPv4 Address of the Computer (A = 32)
   b. AAAA Record – Maps the Domain Name to the corresponding IPv6 Address of the Computer (4A = 128)
   c. NS Record – used for Delegation of a sub domain to group of Name Servers
   d. MX Record – contains the detail of mail server responsible to receive mail for the domain server
   e. TXT Record – Associates some Descriptive Text (about network server or host) with a name
   f. DNSKEY Record – The Flag bit set indicates which Public Key is to be used as Secure Entry Point for the server.

References:
- Wikipedia(https://en.wikipedia.org/wiki/**MX_record**)
- https://tools.ietf.org/html/rfc3757
- https://support.dnsimple.com/articles/ns-record/
- Lecture Slides

10. [12 pts] Describe in detail what each of the following DNS terms are:
    a. DNS Zone Transfer – is to replicate or share multiple copies of DNS databases across a group of DNS Servers (Copy a DNS Server's Record)
    b. Brute Force Forward DNS – Brute force domain names (from any word list) for IP addresses of the respective servers (Iterating through a series of word list – domain names for any hit of IP)
    c. Split DNS – is when the Domain Name resolves to one IP address for internal network and another IP address for external network. (Separating the DNS information that can be accessed by Internal and External Networks)

Reference: Lecture Slides

11. [5 pts] What's the mailing address (snail mail) registered with the domain name facebook.com? How did you find it?
*Facebook MX Record – 10 msgin.vvv.facebook.com
*Used NSLookup – nslookup -type=MX facebook.com

```
Srinivass-MBP:~ darkknight$ nslookup -type=MX facebook.com
Server:         192.168.1.1
Address:    192.168.1.1#53

Non-authoritative answer:
facebook.com        mail exchanger = 10 msgin.vvv.facebook.com.
```

Reference: NSLookup Man Page - http://linux.math.tifr.res.in/manuals/man/nslookup.html

12. [5 pts] What's the IPv6 address associated with the facebook.com? How did you find it? Hint: DNS
*The Ipv6 Address of Facebook is: 2a03:2880:f112:83:face:b00c::25de (used nslookup)
*Used NS Lookup – nslookup -type=aaaa facebook.com

Output:

```
Srinivass-MBP:~ darkknight$ nslookup -type=aaaa facebook.com
Server:         192.168.1.1
Address:    192.168.1.1#53

Non-authoritative answer:
facebook.com    has AAAA address 2a03:2880:f112:83:face:b00c::25de
```

Reference: NSLookup Man Page - http://linux.math.tifr.res.in/manuals/man/nslookup.html

13. [6 pts] According to ARIN, is the IP address 128.122.10.10 allocated to NYU? Explain.

Yes. The Range 128.122.0.0/16 has been allocated to NYU when the domain was registered. ARIN - Registry for Internet number controls IP address of America. NYU has registered with ARIN for IP Addresses. Range allocated to NYU – 128.122.x.x

Reference: https://whois.arin.net/rest/net/NET-128-122-0-0-1

14. [5 pts] Describe the kind of information can be expected to be obtained from using the whois service.

Whois lookup provides the following information:

- Domain Name Owner
- Contact Information – Address and Contact (Email/Phone) of Admin/Tech/Registrant
- Name Servers of the domain
- Dated Record of the activity of the domain name

15. [6 pts] Describe the kind of information can be expected to be obtained from using DNS services only.

DNS Services:

- Domain Name IP Address
- The DNS records (A, AAAA, NS, MX) of the domain
- The Answers from Authoritative and Non-Authoritative servers
- The Root Server Information
- Pointer to reverse DNS Lookup and Domain name aliases
- Host Information and Text regarding the particular domain

16. [10 pts] Describe the steps in the TCP 3-way handshake.

A TCP 3 Way Handshake involves SYN, SYN-ACK and an ACK

- ***TCP SYN*** – A Client initiates a connection to the server with a TCP SYN packet having the SYN bit set - (OPEN)
- ***TCP SYN-ACK*** – The Server acknowledges the Client with a SYN_ACK packet with (SYN and ACK Flag set) - (HALF CONNECT)
- ***TCP ACK or SYN-ACK-ACK*** – The Client responds with an ACK message having the ACK bit set to establish the full connection - (FULL CONNECT)

Reference: Lecture Slides